FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 **FCC DIRECTIVE**	**TITLE** **FCC CYBERSECURITY AND PRIVACY PROGRAMS**	
	Directive Number: **FCCINST 1479.7**	**Effective Date:** **August 11, 2023**

1. PURPOSE: This directive establishes policy and assigns responsibilities for assuring optimal levels of information security and privacy required for Federal Communications Commission (FCC or Commission) information, information systems, and information technology resources.

2. BACKGROUND: This Directive authorizes the FCC's Cybersecurity and Privacy Programs and adopts and incorporates by reference the FCC Cybersecurity and Privacy Policy (CSPP) and the Privacy Program Manual (Manual).[1] Collectively, the Cybersecurity and Privacy Programs require adherence to federal laws and associated requirements governing information security and privacy, and specifically federal policies, procedures, and requirements for the implementation of information security and privacy controls. These controls generally protect against potential security vulnerabilities and breaches by providing safeguards to minimize risks to individuals, information systems, physical property, and other assets. This directive, the CSPP and Manual, will be updated as necessary to reflect changes in relevant federal laws, regulations, guidance, or Executive Orders. They have been drafted in accordance with the FCC's responsibilities to protect information contained in the FCC's information technology systems and will be updated as the security or privacy requirements change in response to new technologies and federal guidance, but not less frequently than annually. The current versions of these documents are available for review on the FCC Intranet.

3. CANCELLATION: This directive replaces FCCINST 1479.6, dated April 2022, and FCCINST 1113.2, dated April 2016.

4. SCOPE AND APPLICABILITY: This directive applies to all FCC Bureaus, Offices, individuals, and staff (i.e., Federal employees, contractor staff, other administrator staff, temporary staff, interns, or volunteers) who access and use FCC information systems or data to conduct Commission business. This directive also applies to all information collected or maintained by, or on behalf of, the FCC and all information systems used or operated by an FCC contractor or administrator.

[1] The Manual, previously styled the Privacy Act Manual, FCCINST 1113.1, contains detailed FCC policies, procedures, and information requirements for implementing the FCC's Privacy Program.

5. AUTHORITIES: Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. § 3551, et seq., as amended;[2] Section 208 of the E-Government Act of 2002, 44 U.S.C. § 3501 note; the Privacy Act of 1974, 5 U.S.C. § 552a; Executive Orders; Office of Management and Budget (OMB) Memoranda and Circulars; and the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications.

6. POLICY: With this directive, the FCC authorizes its Cybersecurity and Privacy Programs in accordance with guidance from OMB.[3] The purpose of these programs is to protect the Confidentiality, Integrity, and Availability (CIA) of information stored and processed in FCC information systems (Federal, Contractor, or administrator managed), supporting FCC's mission, and to ensure that the systems and information are available to authorized users when required. Security and privacy controls are crucial to ensuring the protection and preservation of the CIA[4] of electronic information resources critical to the FCC, the U.S. Government, and the public.

All FCC information and systems shall be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction, whether accidental or intentional, to maintain their CIA. Security and privacy controls that provide this protection shall meet, at a minimum, federal FIPS 199 Moderate security requirements, ensure that FCC information is persistently protected, and promote a defense-in-depth security strategy.

The FCC will follow the NIST Special Publication (SP) 800-37, *Risk Management Framework*, as a starting point that promotes consistent, cost-effective security and privacy standards across all FCC information, systems, and services. NIST SP 800-53 and OMB guidance are used to establish the security and privacy baselines by defining appropriate security and privacy controls to protect FCC information, systems, and services.

All FCC personnel (i.e., Federal employees, contractor staff, other administrator staff, temporary staff, interns, or volunteers) or anyone else with access to federal information and federal information systems[5] shall abide by the programs and policy established by this directive and any other applicable documents to ensure the CIA of all information and information systems.

---

[2] The Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002) was subsequently modified by the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014). As modified, FISMA is codified at 44 U.S.C. § 3551 et seq.

[3] Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016 (OMB Circular A-130).

[4] 44 U.S.C. § 3552(3); OMB Circular A-130.

[5] Federal information system means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. *See* OMB Circular A-130 at 29.

Additionally, it is FCC policy to protect the personally identifiable information (PII) in its possession.[6] All FCC personnel (i.e., Federal employees, contractor staff, other administrator staff, temporary staff, interns, or volunteers) shall be made aware of, and comply with, the Privacy Act and other applicable laws and guidelines addressing privacy. Data about individuals (including PII) shall be collected, maintained, processed, disclosed, and destroyed in accordance with the Privacy Act and other applicable laws and requirements.

All FCC information and information systems must be maintained, stored and secured within the Continental United States (CONUS) and territories. All FCC personnel (i.e., Federal employees, contractor staff, other administrator staff, temporary staff, interns, or volunteers) supporting FCC systems must be able to achieve, at minimum, a High-Risk Public Trust.

7. ROLES & RESPONSIBILITIES: The following is a brief overview of the roles and responsibilities related to the Cybersecurity and Privacy Programs. A full description of these responsibilities is contained in the CSPP, the Privacy Program Manual, and other specific cybersecurity and privacy policies including "*Responding to a PII Breach*," the FCC's standard operating procedure (Breach SOP) for responding to a PII breach.

   A. The FCC Chairperson shall, in consultation with the Managing Director and the General Counsel, designate the Senior Agency Official for Privacy (SAOP) within the Office of General Counsel; the SAOP shall have agency-wide responsibility to ensure compliance with federal laws, regulations, and policies relating to information privacy.

   B. The Managing Director shall oversee the management of the FCC Cybersecurity and Privacy Programs.

   C. The FCC Chief Information Officer (CIO) shall share overall responsibility for the Cybersecurity and Privacy Programs with the SAOP and shall have primary responsibility for overseeing the development and maintenance of a Commission-wide information security program. The CIO shall preserve and protect PII contained in FCC information systems; collaborate with the SAOP to safeguard information maintained or transmitted by an information system; and assist the Bureaus and Offices in the implementation of uniform and consistent policies and standards governing the acquisition, maintenance, and use of information systems and information technology. The CIO shall establish training programs for FCC personnel and contractors to ensure ongoing compliance with information security laws, regulations, policies, and procedures. The CIO shall provide Bureau/Office

[6] Under applicable federal guidance, PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. OMB Circular A-130 at 33.

(B/O) Chiefs, Information Owners, System Owners, and FCC System Users with Standard Operating Procedures (e.g. step-by-step instructions with process milestones and timelines, and roles and responsibilities defined, for implementing FCC information systems) to carry out their responsibilities under this Directive, including at the commencement of developing new information technology systems. The CIO will allocate adequate IT staff and contractor resources to guide and assist B/O Chiefs, Information Owners, System Owners, and FCC System Users. The CIO will ensure that IT staff and contractors provide adequate customer service to B/O Chiefs, Information Owners, System Owners, and FCC System Users. The CIO will ensure that IT staff and contractors coordinate with each other and all entities listed under Roles and Responsibilities to ensure timely completion of assigned activities.

D. The FCC Chief Information Security Officer (CISO) shall carry out the CIO's responsibilities under FISMA, with information security as their primary duty, and shall head a division with the required mission and resources to assist in achieving and maintaining organizational compliance with FCC and federal government information security policies, standards and procedures.

E. The FCC SAOP shall share overall responsibility for the privacy components referenced in the Cybersecurity and Privacy Programs with the CIO and shall be primarily responsible for developing, implementing, and maintaining a Commission-wide privacy program to ensure compliance with all applicable laws and regulations regarding the collection, processing, maintenance, disclosure, and disposal of PII and to manage privacy risks. The FCC SAOP shall provide guidance to the FCC Chairperson, Commissioners, and senior leadership on privacy issues. The SAOP shall coordinate with the CIO, CISO, and the B/O Chiefs to ensure that, while still fulfilling its missions and functions, the FCC is limiting the collection, processing, maintenance, and disclosure of PII to the minimum necessary; avoiding the use of PII in nonproduction environments; and addressing privacy risks at the design stage when acquiring, developing, or modifying information systems. Consistent with the FCC Privacy Program Manual, the SAOP shall chair the FCC Data Integrity Board (DIB) that oversees information sharing, computer matching, and related issues; review and approve all FIPS-199 categorizations, System of Records Notices (SORNs), Initial Privacy Assessments (IPAs), and Privacy Impact Assessments (PIAs); ensure that all FCC personnel (i.e., Federal employees, contractor staff, other administrator staff, temporary staff, interns, or volunteers) receive appropriate training and education regarding privacy laws, regulations, policies, and procedures governing the agency's handling of PII; play a central policymaking role in the Commission's development and evaluation of legislative, regulatory, and related policy proposals implicating privacy issues; and coordinate the agency's response to PII breaches under the Breach SOP.

F. The FCC Privacy Team shall be comprised of the SAOP, attorney advisors from the Office of General Counsel, and the Privacy Analyst. The Privacy Team shall

be responsible for ensuring ongoing compliance with federal laws, regulations, and policies relating to privacy; providing training and education regarding privacy laws, regulations, policies, and procedures governing the collection, processing, maintenance, disclosure, and disposal of PII; drafting and negotiating Computer Matching Agreements (CMAs) with federal and state entities and satisfying all requirements related to the FCC DIB; drafting, altering, amending, and updating SORNs; reviewing FIPS-199s, IPAs, and PIAs for information systems; reviewing Commission items for privacy issues; reviewing contracts that involve the collection, processing, maintenance, disclosure, and disposal of PII; responding to requests under the Privacy Act; supporting the agency's response to PII breaches; and coordinating the submission of required documents (e.g., submitting SORNs to the Office of Management and Budget, and Congress for advance review and for publication in the *Federal Register*).

G. The FCC B/O Chiefs shall ensure that Information Owners, System Owners, and Business Owners within their B/Os perform their delegated roles and responsibilities and keep the CIO and SAOP apprised of changes in the collection, processing, maintenance, disclosure, or disposal of information, or the acquisition of new information, information systems, or information technology resources.

H. The Information Owner or Information Steward shall be the individual or group that helps to ensure the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance. The information owner or information steward may not be tied to a particular Bureau or Office; the role may vary by information system.

I. Information System Security Officers (ISSOs) shall collaborate with System Owners and the SAOP to assist with the completion of privacy documentation required for an Authority to Operate (ATO) such as FIPS-199 categorizations, IPAs, and, if necessary PIAs. The ISSO may not be tied to a particular Bureau or Office; the role may vary by information system. ISSOs shall collaborate with the System Owners and Information Owner(s) for ensuring that the security and privacy posture is maintained for an organizational system and works in close collaboration with the system owner. ISSOs serve as the principal advisors on all matters, technical and otherwise, involving the controls for systems and have the knowledge and expertise to manage the security or privacy aspects of organizational systems. ISSOs shall be responsible for the day-to-day system security and privacy operations including developing and updating security and privacy plans, managing and controlling changes to the system, and assessing the security or privacy impact of those changes.

J. System Owner shall be the official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner may not be tied to a particular Bureau or Office; the role may vary by information system. The system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements) and for ensuring compliance with security requirements. In coordination with the ISSOs and Privacy Team, the system owner is responsible for the development and maintenance of the security and privacy plans and ensures that the system is operated in accordance with the selected and implemented controls. The system owner ensures that system users and support personnel receive the requisite security and privacy training. Based on guidance from the authorizing official, the system owner informs organizational officials of the need to conduct the authorization, ensures that resources are available for the effort, and provides the required system access, information, and documentation to control assessors. The system owner receives the security and privacy assessment results from the control assessors. After taking appropriate steps to reduce or eliminate vulnerabilities or security and privacy risks, the system owner assembles the authorization package and submits the package to the authorizing official or the authorizing official designated representative for adjudication.

K. Business Owner shall be the senior official or executive within an organization with specific mission or line of business responsibilities and shall have a security or privacy interest in the organizational systems supporting those missions or lines of business. The business owner may not be tied to a particular Bureau or Office; the role may vary by information system. Business owners shall be key stakeholders that have a significant role in establishing organizational mission and business processes and the protection needs and security and privacy requirements that ensure the successful conduct of the organization's missions and business operations.

L. Enterprise Acquisition Center shall ensure that proposed solicitations and contracts that involve the collection, use, processing, maintenance, or disclosure of PII are reviewed in advance by the SAOP; ensure inclusion of appropriate clauses concerning the protection of PII and compliance with applicable laws, regulations, requirements, and directives are included in solicitations and contracts; assist the SAOP with procuring identity theft protection/monitoring in the event that the Chairperson has approved such measures in response to a PII breach; provide contract management; and ensure Contracting Officer Representatives conduct oversight of contractor compliance with FCC privacy requirements.

M. The FCC System Users are FCC personnel who must adhere to agency policies, including those described in section 8 of this Directive, "Rules of Behavior," as well as staying up to date on changes to those policies and directives.

8. Rules of Behavior: The Privacy Act of 1974, FISMA, OMB A-123 and A-130 mandate that federal agencies maintain Rules of Behavior (RoB) for using federal systems. Prior to obtaining access to FCC systems, all personnel, including contractors and others working on behalf of the FCC, must agree to the FCC's RoB. The RoB delineate responsibilities and expected behavior of all individuals with access to FCC systems and state the consequences of non-compliance. The CIO and the SAOP shall define and maintain enterprise wide RoB that can be used for all information systems. The RoB shall be reviewed and updated as necessary, but not less than annually. FCC OCIO shall ensure that users requesting access to FCC systems complete Cybersecurity Awareness Training and sign the FCC RoB.

9. EFFECTIVE DATE AND IMPLEMENTATION: This directive is effective immediately and shall be implemented promptly upon distribution.

MARK STEPHENS
Digitally signed by MARK STEPHENS
Date: 2023.08.11 09:49:56 -04'00'

Mark Stephens
Managing Director